(12) UK Patent Application (19) GB (11) 2 356 469 (13) A

(43) Date of A Publication 23.05.2001

(21) Application No 9927031.6

(22) Date of Filing 17.11.1999

(51) INT CL[7]
G06F 1/00

(52) UK CL (Edition S)
G4A AAP
U1S S2120

(56) Documents Cited
WO 87/07061 A1 US 4891506 A

(58) Field of Search
UK CL (Edition R) G4A AAP AFGN
INT CL[7] G06F 1/00
ONLINE WPI EPODOC PAJ

(71) Applicant(s)
Motorola Limited
(Incorporated in the United Kingdom)
Jays Close, Viables Industrial Estate, BASINGSTOKE, Hampshire, RG22 4PD, United Kingdom

Motorola Australia PTY Ltd
(Incorporated in Australia - Victoria)
6 Caribbean Drive, Scoresby, Victoria 3179, Australia

(72) Inventor(s)
Jeremy Stephen Philip Webber
Paul Lachlan Arnott
Peter McGinn
Mitchell Ross
Peter Galbraith

(74) Agent and/or Address for Service
Sarah Gibson
Motorola Limited, European Intellectual Property Department, Midpoint, Alencon Link, BASINGSTOKE, Hampshire, RG21 7PL, United Kingdom

(54) Abstract Title
Portable data carrier memory management system and method

(57) A portable data carrier 1 (eg. ic card, smart card, chip card) includes a processor 2 having privileged 3 and non-privileged 4 modes of operation. A memory 10 is divided into a plurality of pages 11, 12, 13, 14, each page having one of a predetermined number of security levels associated therewith. A Memory Management Unit (MMU) 5 is coupled to the processor 2 and to the memory 10 to control access of the processor 2 to the pages of the memory according to the security level of the page that the memory is trying to access. In privileged mode the processor unit 2 can set control register 6 in the MMU 5 and thus alter the security levels associated with each page of memory. In the given embodiment a hardwire switch 7 is used to determine the operating mode of the processor. The memory may consist of RAM, ROM and/or EPROM.

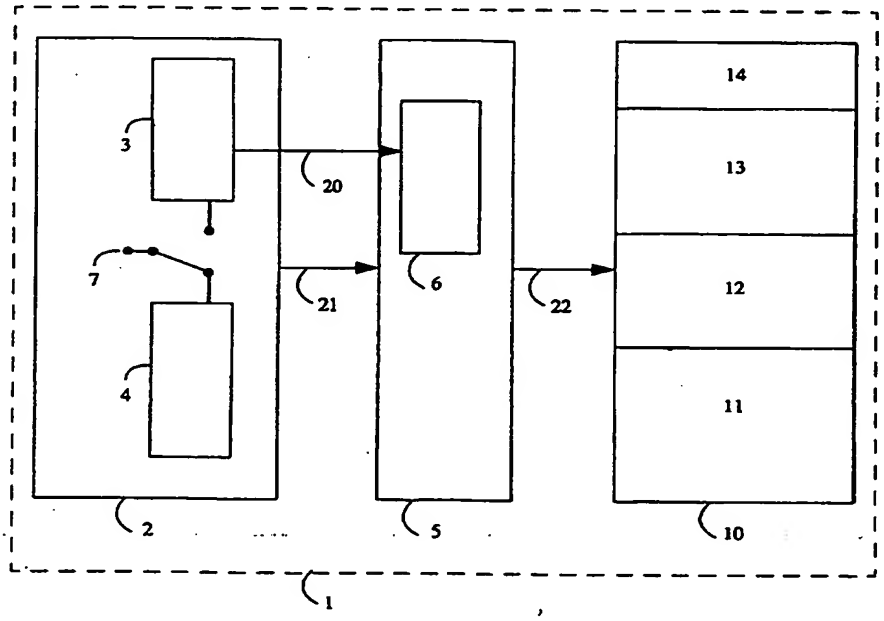

FIG. 1

GB 2 356 469 A

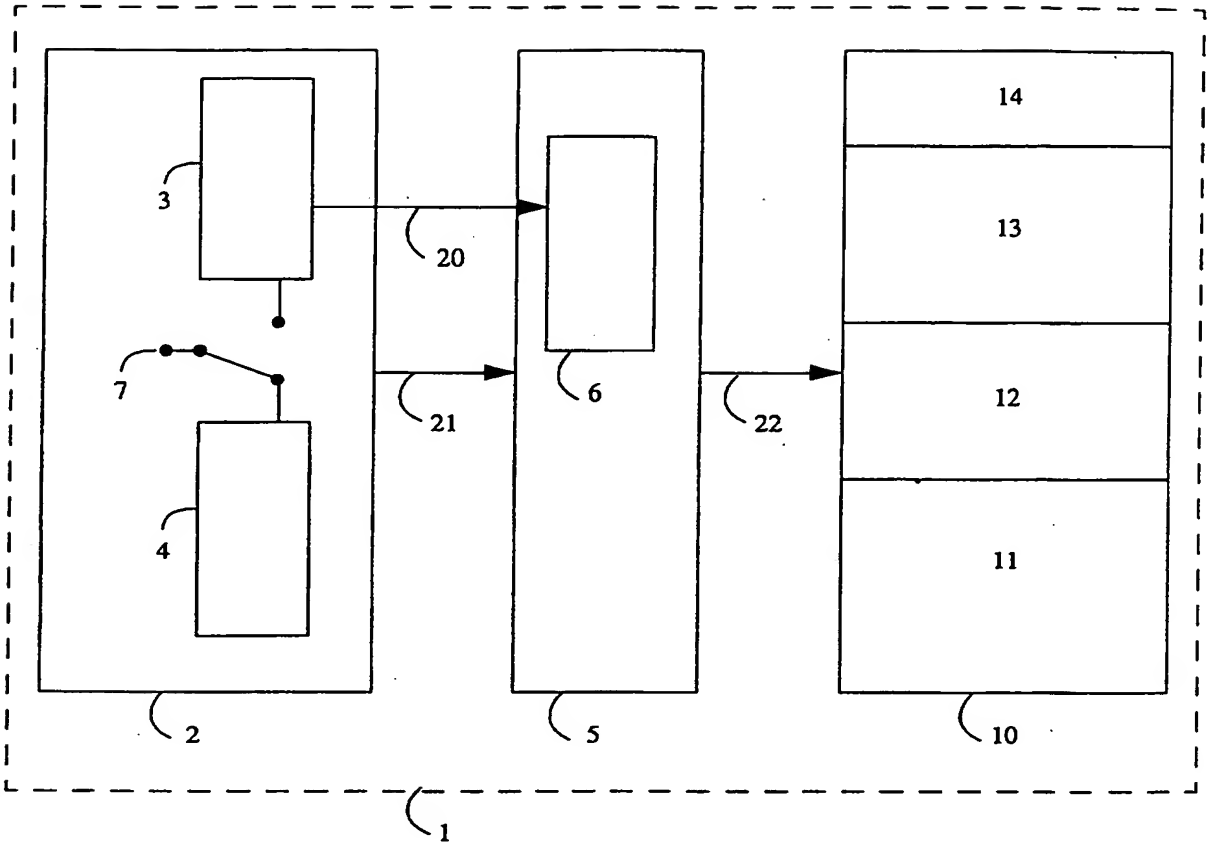

FIG. 1

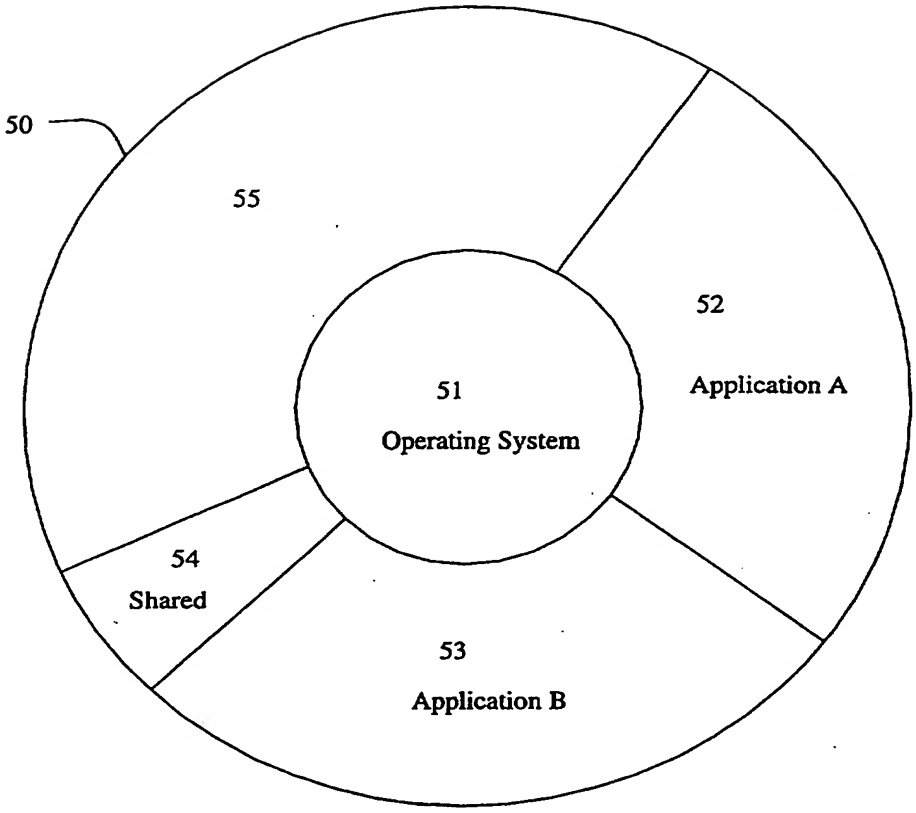
50
55
52
Application A
51
Operating System
54
Shared
53
Application B

FIG. 2

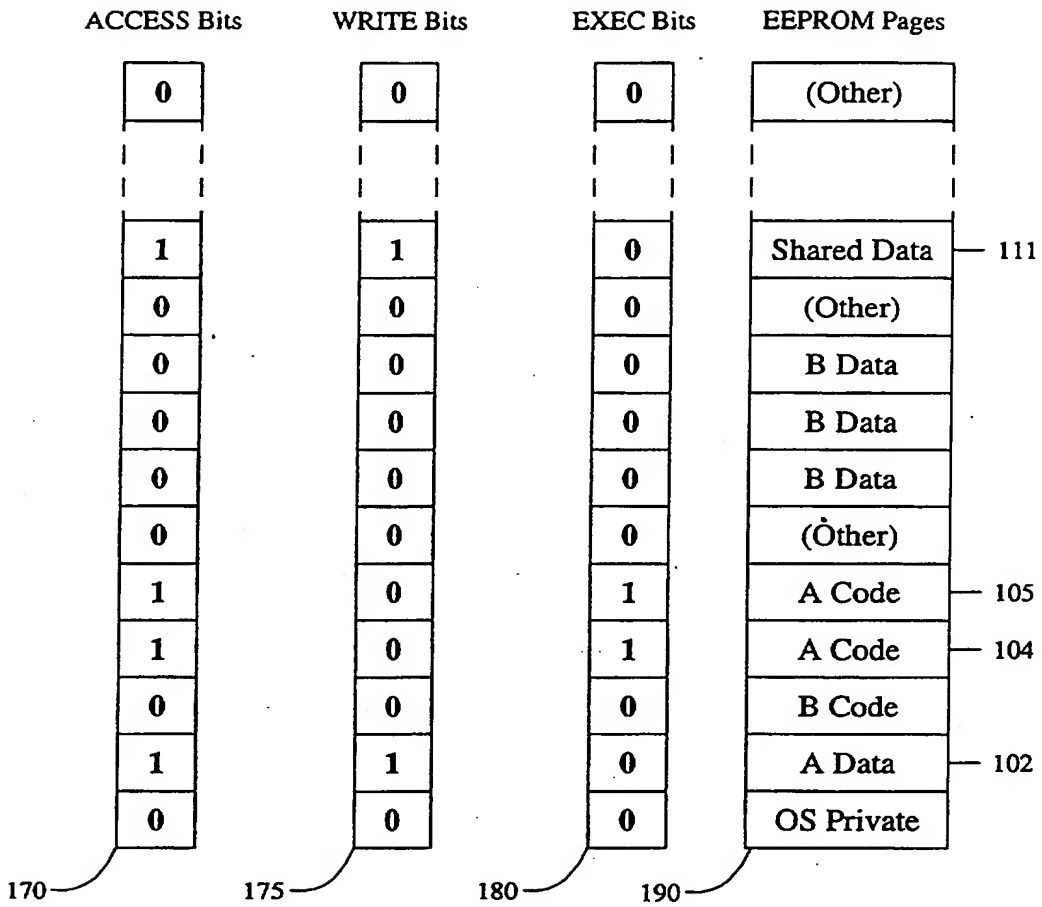
ACCESS Bits
WRITE Bits
EXEC Bits
EEPROM Pages
0
0
0
(Other)
1
1
0
Shared Data
111
0
0
0
(Other)
0
0
0
B Data
0
0
0
B Data
0
0
0
B Data
0
0
0
(Other)
1
0
1
A Code
105
1
0
1
A Code
104
0
0
0
B Code
1
1
0
A Data
102
0
0
0
OS Private
170
175
180
190

FIG. 3

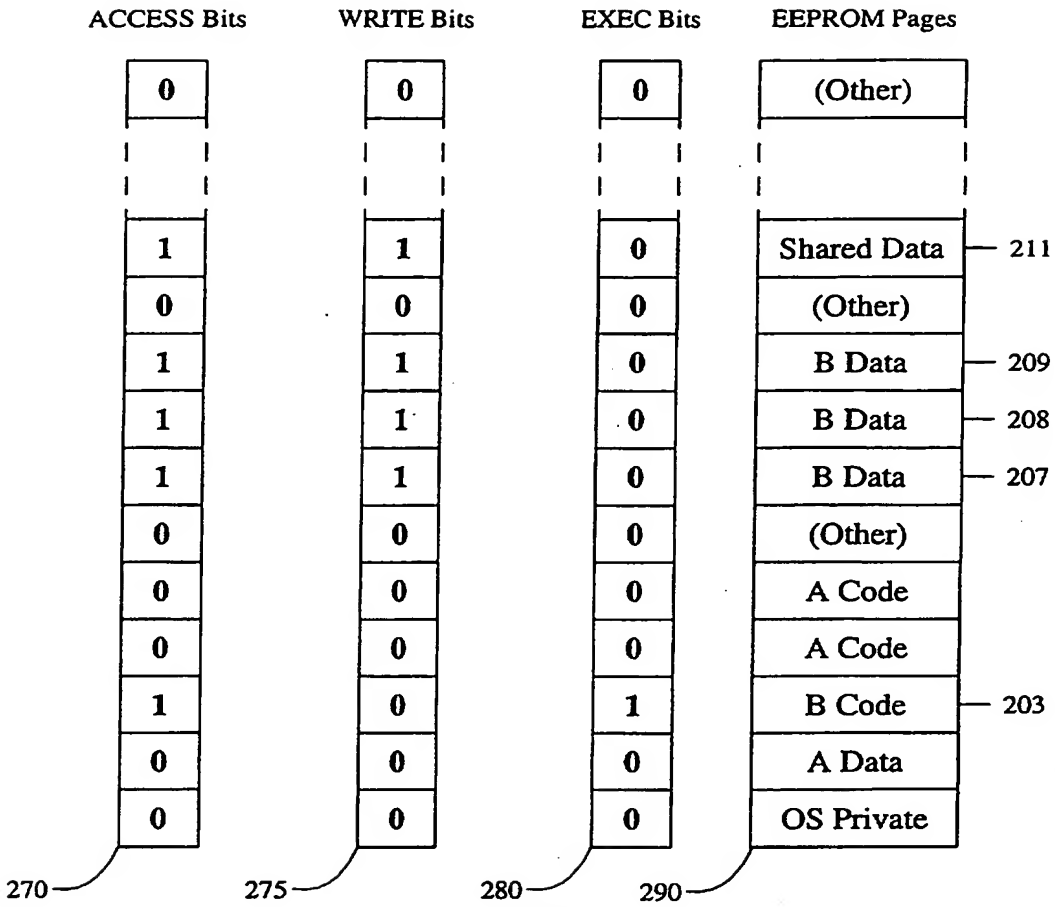
ACCESS Bits
WRITE Bits
EXEC Bits
EEPROM Pages
0
0
0
(Other)
1
1
0
Shared Data
211
0
0
0
(Other)
1
1
0
B Data
209
1
1
0
B Data
208
1
1
0
B Data
207
0
0
0
(Other)
0
0
0
A Code
0
0
0
A Code
1
0
1
B Code
203
0
0
0
A Data
0
0
0
OS Private
270
275
280
290

FIG. 4

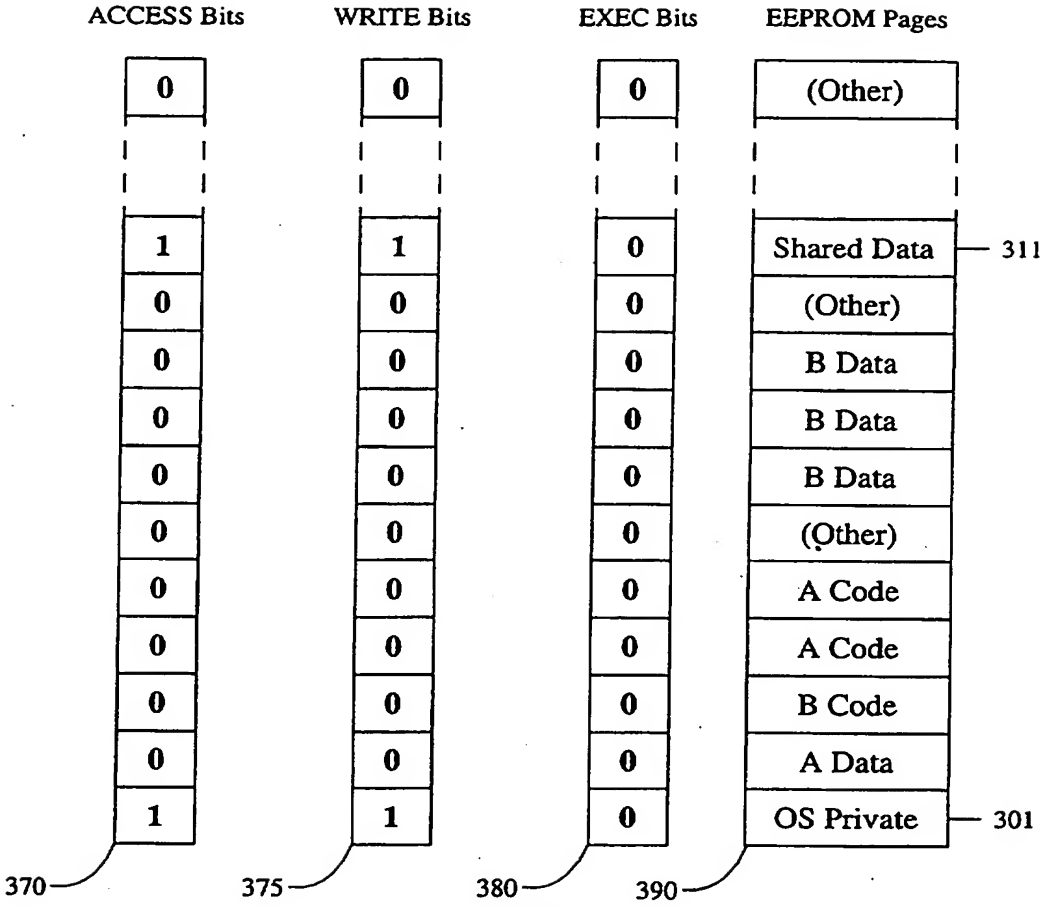
ACCESS Bits
WRITE Bits
EXEC Bits
EEPROM Pages
0
0
0
(Other)
1
1
0
Shared Data
311
0
0
0
(Other)
0
0
0
B Data
0
0
0
B Data
0
0
0
B Data
0
0
0
(Other)
0
0
0
A Code
0
0
0
A Code
0
0
0
B Code
0
0
0
A Data
1
1
0
OS Private
301
370
375
380
390

FIG. 5

Portable Data Carrier Memory Management System and Method

Field of the Invention

This invention relates to a method and apparatus for managing a memory in a portable data carrier.

Background of the Invention

Conventional portable data carriers (e.g. smartcards or chip cards) often have more than one software application loaded thereon, such as different banks' account access software, personal data, electronic purse, or other applications, each application having a security function associated with it. The applications are stored in a memory on a chip in the smartcard, on which chip are usually also located the processor which controls the operation of the smartcard, and other electronic circuits providing other functionality.

Different applications may well have different security levels and, even within each application, different parts of the application and different data may have different security levels. Thus, different parts of the memory need to have different security levels to allow or restrict access thereto.

Brief Summary of the Invention

The present invention therefore seeks to provide a method and apparatus for managing a memory in a portable data carrier which overcome, or at least reduce the above-mentioned problems of the prior art.

Accordingly, in one aspect, the invention provides a portable data carrier comprising a processor having privileged and non-privileged modes of operation, a memory divided into a plurality of blocks, each block having one of a predetermined number of security levels associated therewith, and a Memory Management Unit (MMU) coupled to the processor and to the memory to control access of the processor to the memory according to the mode in which the processor is operating and the security level of the memory block that the memory is trying to access.

Preferably, the blocks into which the memory is divided are pages and the MMU is a Paged Memory Management Unit (PMMU).

In a preferred embodiment, the PMMU restricts access of the processor to the pages of the memory when the processor is operating in the non-privileged mode to only those pages that have a predetermined subset of the predetermined number of security levels.

Preferably, the predetermined number of security levels is five, a first security level allowing access to the page of memory or not, a second security level allowing reading of the page of memory or not, a third security level allowing reading and writing

of the page of memory or not, a fourth security level allowing reading and executing of the page of memory or not, and a fifth security level allowing reading, writing and executing of the page of memory or not.

The processor preferably includes a hardware switch for switching between the privileged and non-privileged operating modes.

In one embodiment, the PMMU comprises at least one register having a plurality of bits, each bit corresponding to a page of the memory, a bit value of each bit providing an indication of the security level of the corresponding page.

Preferably, the PMMU comprises at least three registers, a first register having a plurality of bits whose bit values indicate whether the corresponding page of the memory can be accessed or not, a second register having a plurality of bits whose bit values indicate whether the corresponding page of the memory can be written to or not, and a third register having a plurality of bits whose bit values indicate whether the corresponding page of the memory can be executed to or not.

Preferably, bits in the second and third registers are only utilised if the bits in the first register corresponding to the same page have bit values indicating that the page can be accessed.

The memory can comprise an Electrically Erasable Programmable Read Only Memory (EEPROM), a Random Access Memory (RAM) and/or a Read Only Memory (ROM).

According to a second aspect, the invention provides a method of managing a memory in a portable data carrier also including a processor and a Paged Memory Management Unit, the memory being divided into a plurality of pages, the method comprising the steps of entering a privileged mode of operation of the processor, writing one of a plurality of predetermined security levels in the PMMU for at least one of the pages of the memory, exiting the privileged mode of operation of the processor, entering a non-privileged mode of operation of the processor, requesting access to at least one page of the memory by the processor to the PMMU, utilising the PMMU to determine the security level of the at least one page in the memory to which the processor has requested access, selectively accessing the at least one page of memory based on the security level determined by the PMMU, and exiting the non-privileged mode of operation of the processor.

In a preferred embodiment, the step of selectively accessing the at least one page of memory comprises accessing the at least one page of memory when the security level of the page is within a predetermined subset of the predetermined number of security levels.

Preferably, the predetermined number of security levels is five, a first security level allowing access to the page of memory or not, a second security level allowing reading of the page of memory or not, a third security level allowing reading and writing of the page of memory or not, a fourth security level allowing reading and executing of the page of memory or not, and a fifth security level allowing reading, writing and executing of the page of memory or not.

The steps of entering and exiting the privileged and non-privileged modes of operation of the processor preferably comprise utilising a hardware switch in the processor.

In one embodiment, the step of writing one of a plurality of predetermined security levels in the PMMU comprises setting a bit value of a bit in at least one register in the PMMU for each page of the memory for which a security level is to be written.

Preferably, the step of writing one of plurality of predetermined security levels in the PMMU comprises setting a bit value of a corresponding bit in each of three registers in the PMMU for each page of the memory for which a security level is to be written, the bits in a first register indicating whether the corresponding page of the memory can be accessed or not, the bits in a second register indicating whether the corresponding page of the memory can be written to or not, and the bits in a third register indicating whether the corresponding page of the memory can be executed to or not.

The step of utilising the PMMU to determine the security level preferably comprises utilising the bit in the first register corresponding to the at least one page to be accessed, and only utilising the corresponding bits in the second and third registers if the bit value of the bit in the first register indicates that the page can be accessed.

Brief Description of the Drawings

One embodiment of the invention will now be more fully described, by way of example, with reference to the drawings, of which:

FIG. 1 shows a smartcard chip having a number of components and logical access channels between those components;

FIG. 2 shows a conceptual representation of the contents of a memory in the smartcard chip of FIG. 1, with a division of access between an operating system and various applications stored in the memory; and

FIGS. 3, 4 and 5 show examples of a control mechanism for managing the memory in the smartcard chip of FIG. 1.

Detailed Description of the Drawings

As shown in FIG. 1, in one embodiment of the present invention, a smartcard chip 1 includes a number of physical components, which are shown schematically as a

processing unit 2, a memory management unit 5 and a memory unit 10. The processing unit 2 is used to execute programs which are stored in the memory unit 10.

A stored program may cause the processing unit 2 to access data, which is also contained in the memory unit 10. All accesses from the processing unit 2 to the memory unit 10 must occur via the memory management unit 5, via channels 21 and 22 in FIG. 1. Thus, no physical access paths exist directly from the processing unit 2 to the memory unit 10.

Among its capabilities, the processing unit 2 has two operating modes. In a more privileged mode 3, the processing unit 2 is allowed to set control registers 6 in the memory management unit 5 using a relatively secure channel 20 and in a less privileged mode 4, the processing unit 2 is not allowed to alter the way the memory management unit 5 operates, but can only access the memory unit 10 via the channels 21 and 22. A hardware switch 7 is provided within the processing unit 2 to switch between the more privileged and less privileged modes.

The memory unit 10 is divided into blocks, or pages, 11, 12, 13 and 14. When the processing unit 2 accesses the memory it must specify the page of memory to be accessed, and the type of access required. The memory management unit 5, which can be a so-called Paged Memory Management Unit (PMMU), can then grant or deny access based on whether its control registers permit the processing unit 2 to have the requested type of access at that particular point of time.

It will be appreciated that because it is possible for a program operating in the more privileged mode to modify the control registers of the PMMU 5, this form of access control is only effective when the processing unit 2 is operating in the less privileged mode.

Although FIG. 1 shows the memory unit 10 divided into four pages, it will be appreciated that the present invention applies to a memory unit divided into a number of blocks, not necessarily only four.

FIG. 2 shows a practical example of the use of the memory unit 10 of FIG. 1. In FIG. 2, a memory 50 is depicted in an "onion" diagram. At the centre of the diagram is a page of memory 51 which is private to the operating system. The operating system is able to execute in the more privileged mode of the processing unit 2, and thus is able to access the whole of memory 50, in addition to its private page 51. In addition to the operating system, there are two applications, called "A" and "B". Application A has access to a particular page of memory 52 and application B has access to another block of memory 53. A further block of memory 54 is accessible to both applications A and B. The remainder of memory 55 is free or used by other applications.

FIGS. 3, 4 and 5 show an operational scenario in which the smart card chip described above with reference to FIG. 1 possessing the memory described above with reference to FIG. 2 can be used to implement paged memory protection. The memory can consist of a Random Access Memory (RAM), a Read-Only Memory (ROM), an Electronically Erasable Programmable Read-Only Memory (EEPROM), or any other type of memory which is divided into pages, which can have different security levels associated therewith.

For example, the smartcard chip can be implemented having an M-Core processor core, together with a PMMU and RAM, ROM and EEPROM memory, together with a set of device registers providing control of the PMMU, as manufactured by Motorola, Inc.

Thus, as shown in FIGS. 3, 4 and 5, the PMMU contains a set of three registers 170, 175 and 180 in FIG. 3, 270, 275 and 280 in FIG. 4, and 370, 375 and 380 in FIG. 5, which control access to the EEPROM pages 190, 290 and 390, respectively, of the memory. Each of the registers consists of 64 bits, with each bit being associated with a particular page in the EEPROM memory portion. It will be appreciated that the size of the register depends on the number of pages into which the portion is divided. Each portion of memory of a different type will have its own set of registers, but, for clarity, only one set controlling access to the EEPROM memory portion is shown.

The first register is an "Access" register, which provides a first level of security either allowing or restricting access to the particular pages of the memory. If the bit value for a particular page is "1", access is granted to that page, but if the bit value is "0", access is denied.

The next register is a "Write" register, which provides a second level of security either allowing or denying write operations to the particular pages of memory. Thus, if the bit value for a particular page is "1" then both read (access) and write operations are permitted on that page. If the bit value is "0", then write operation are not permitted, but read (access) operations are permitted on that page. These operations are only permitted if access to the page has been granted by the EEPROM "Access" register.

The third register is an "Execute" register providing a third level of security either allowing or restricting execute operations to be performed on the code on the particular page. If the bit value for a particular page is "1" then native code may execute from that page. However, if the bit value is "0", native code may not execute from that page. Again, execution is only permitted if access to the page has been granted by the EEPROM "Access" register.

Each of FIGS. 3, 4 and 5 show the PMMU registers at a particular moment in time providing up to five different levels of security in total for the pages of the EEPROM memory.

FIG. 3 shows the state of the registers when an Application A has control of the processor. By looking at which bits in the "Access" register 170 have values of "0" or "1", the access rights to particular pages in the EEPROM memory 190 can be determined. Thus, as shown, "Access" register 170 specifies that Application A can read from pages containing application A data, in this case only one such page 102 being shown, pages 104 and 105 having application A code and one or more pages 111 having shared data. None of the other pages in the memory 190 cannot be accessed by the processor.

The "Write" register 175 specifies which of the accessible pages, as determined from the "Access" register 170, can be written to. Thus, as shown, application A can write to the page 102 containing application A data and to the page 111 containing shared data, but not to the pages 104 and 105 containing application A code. Similarly, the "Execute" register 180 specifies which of the accessible pages, as determined from the "Access" register 170, can be executed. Thus, as shown, the pages 104 and 105 containing application A code are the only pages permitted to execute.

Any other form of access will cause an exception, returning control to the operating system. Thus, application B does not have to "trust" application A, in order for them both to occupy the same smartcard securely. Any failure or even deliberate corruption of application A cannot affect application B, except through the defined shared data page 111.

FIG. 4 shows the state of the registers when application B has control. In this case, the "Access" register 270 specifies that the application B can access page(s) 203 containing application B code, the pages 207, 208 and 209 containing application B data and the page 211 containing shared data. The "Write" register 275 specifies that, of the pages that application B can access, the application can write to the pages 207, 208 and 209 containing application B data and to page 211 containing shared data, but not to page 203 containing application B code. Similarly, the "Execute" register 280 specifies that, of the pages that application B can access, the application can only execute the page 203 containing application B code.

Again, any other form of access will cause an exception, meaning that application A does not have to "trust" application B.

Finally, FIG. 5 shows the state of the registers when a less privileged portion of the operating system, such as an unprivileged service routine has control. In this case, the "Access" register 370 and the "Write" register 375 specify that the unprivileged

service routine can read from and write to page 301 containing operating system private data and page 311 containing shared data, but no access to other portions of the memory is allowed. The "Access" register 370 and the "Execute" register 380 specify that the unprivileged service routine cannot execute any pages in the memory 390.

Thus, the applications do not have to "trust" this portion of the operating system. Clearly, because it can update the PMMU registers, the more privileged portion of the operating system can read from, write to and execute any portion of memory, and thus has to be "trusted" by all applications.

The embodiment of the invention described above therefore provides a mechanism whereby different applications or different parts of an application which execute on a smartcard chip have limited access to various sections of memory based on the security level of the application or part thereof and the security level of the section of memory being accessed.

It will be appreciated that although only one particular embodiment of the invention has been described in detail, various modifications and improvements can be made by a person skilled in the art without departing from the scope of the present invention. For example, although the embodiment described above has three registers providing up to five levels of security:

1. No Access;
2. Read Only;
3. Read and Write;
4. Read and Execute;
5. Execute, Read and Write,

different numbers of security levels can easily be provided by providing different numbers of registers.

Claims

1. A portable data carrier comprising:

a processor having privileged and non-privileged modes of operation;

a memory divided into a plurality of blocks, each block having one of a predetermined number of security levels associated therewith; and

a Memory Management Unit (MMU) coupled to the processor and to the memory to control access of the processor to the memory according to the mode in which the processor is operating and the security level of the memory block that the processor is trying to access.

2. A portable data carrier according to claim 1, wherein the blocks into which the memory is divided are pages and the MMU is a Paged Memory Management Unit (PMMU).

3. A portable data carrier according to claim 2, wherein the PMMU restricts access of the processor to the pages of the memory when the processor is operating in the non-privileged mode to only those pages that have a predetermined subset of the predetermined number of security levels.

4. A portable data carrier according to claim 3, wherein the predetermined number of security levels is five, a first security level allowing access to the page of memory or not, a second security level allowing reading of the page of memory or not, a third security level allowing reading and writing of the page of memory or not, a fourth security level allowing reading and executing of the page of memory or not, and a fifth security level allowing reading, writing and executing of the page of memory or not.

5. A portable data carrier according to claim 1, wherein the processor includes a hardware switch for switching between the privileged and non-privileged operating modes.

6. A portable data carrier according to claim 2, wherein the PMMU comprises at least one register having a plurality of bits, each bit corresponding to a page of the memory, a bit value of each bit providing an indication of the security level of the corresponding page.

7. A portable data carrier according to claim 6, wherein the PMMU comprises at least three registers, a first register having a plurality of bits whose bit values indicate whether the corresponding page of the memory can be accessed or not, a second register having a plurality of bits whose bit values indicate whether the corresponding page of the memory can be written to or not, and a third register having a plurality of bits whose bit values indicate whether the corresponding page of the memory can be executed to or not.

8. A portable data carrier according to claim 7, wherein bits in the second and third registers are only utilised if the bits in the first register corresponding to the same page have bit values indicating that the page can be accessed.

9. A portable data carrier according to claim 1, wherein the memory comprises an Electrically Erasable Programmable Read Only Memory (EEPROM).

10. A portable data carrier according to claim 1, wherein the memory comprises a Random Access Memory (RAM).

11. A portable data carrier according to claim 1, wherein the memory comprises a Read Only Memory (ROM).

12. A method of managing a memory in a portable data carrier also including a processor and a Paged Memory Management Unit, the memory being divided into a plurality of pages, the method comprising the steps of:

entering a privileged mode of operation of the processor;

writing one of a plurality of predetermined security levels in the PMMU for at least one of the pages of the memory;

exiting the privileged mode of operation of the processor;

entering a non-privileged mode of operation of the processor;

requesting access to at least one page of the memory by the processor to the PMMU;

utilising the PMMU to determine the security level of the at least one page in the memory to which the processor has requested access;

selectively accessing the at least one page of memory based on the security level determined by the PMMU; and

exiting the non-privileged mode of operation of the processor.

13. A method of managing a memory according to claim 12, wherein the step of selectively accessing the at least one page of memory comprises:

accessing the at least one page of memory when the security level of the page is within a predetermined subset of the predetermined number of security levels.

14. A method of managing a memory according to claim 13, wherein the predetermined number of security levels is five, a first security level allowing access to the page of memory or not, a second security level allowing reading of the page of memory or not, a third security level allowing reading and writing of the page of memory or not, a fourth security level allowing reading and executing of the page of memory or not, and a fifth security level allowing reading, writing and executing of the page of memory or not.

15. A method of managing a memory according to claim 12, wherein the steps of entering and exiting the privileged and non-privileged modes of operation of the processor comprise utilising a hardware switch in the processor.

16. A method of managing a memory according to claim 13, wherein the step of writing one of a plurality of predetermined security levels in the PMMU comprises setting a bit value of a bit in at least one register in the PMMU for each page of the memory for which a security level is to be written.

17. A method of managing a memory according to claim 15, wherein the step of writing one of plurality of predetermined security levels in the PMMU comprises setting a bit value of a corresponding bit in each of three registers in the PMMU for each page of the memory for which a security level is to be written, the bits in a first register indicating whether the corresponding page of the memory can be accessed or not, the bits in a second register indicating whether the corresponding page of the memory can be written to or not, and the bits in a third register indicating whether the corresponding page of the memory can be executed to or not.

18. A method of managing a memory according to claim 17, wherein the step of utilising the PMMU to determine the security level comprises:

utilising the bit in the first register corresponding to the at least one page to be accessed; and

only utilising the corresponding bits in the second and third registers if the bit value of the bit in the first register indicates that the page can be accessed.

19. A portable data carrier substantially as hereinbefore described with reference to the accompanying drawings.

20. A method of managing a memory in a portable data carrier substantially as hereinbefore described with reference to the accompanying drawings.

Application No: GB 9927031.6
Claims searched: ALL
Examiner: Russell Maurice
Date of search: 6 June 2000

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.R): G4A (AAP, AFGN)

Int Cl (Ed.7): G06F (1/00)

Other: Online WPI EPODOC PAJ

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
A	WO 87/07061 A	AT&T (see abstract and Fig 2.)	-
A	US 4891506 A	Yoshimatsu (see whole document)	-

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.